Software Rights Archive, LLC v. Google Inc. et al Doc. 123

Ronald L. Motley, Esq. (SC Bar No. RM-2730)
Jodi Westbrook Flowers, Esq. (SC Bar No. 66300)
Donald Migliori, Esq. (RI Dar No. 4963;
MA Bar No. 567562; and MN Bar No. 0245951)
Vincent I. Parrett (CA Bar No. 237563)
**MOTLEY RICE LLC**
28 Bridgeside Boulevard
P.O. Box 1792
Mount Pleasant, South Carolina 29465
Telephone: (843) 216-9000
Facsimile: (843) 216-9027
MDL1791@motleyrice.com

**INTERIM CLASS COUNSEL**

**UNITED STATES DISTRICT COURT**

**FOR THE NORTHERN DISTRICT OF CALIFORNIA**

**SAN FRANCISCO DIVISION**

| | |
|---|---|
| IN RE NATIONAL SECURITY AGENCY TELECOMMUNICATIONS RECORDS LITIGATION, MDL No. 1791<br><br>This Document Relates To:<br><br>ALL CASES BROUGHT AGAINST DEFENDANTS TRANSWORLD NETWORK CORP., COMCAST TELECOMMUNICATIONS, INC., T-MOBILE USA, INC., AND MCLEODUSA TELECOMMUNICATIONS SERVICES, INC. | MDL Docket No 06-1791 VRW<br><br>**CLASS ACTION**<br><br>**MASTER CONSOLIDATED COMPLAINT AGAINST DEFENDANTS TRANSWORLD NETWORK CORP., COMCAST TELECOMMUNICATIONS, INC., T-MOBILE USA, INC., AND MCLEODUSA TELECOMMUNICATIONS SERVICES, INC., FOR DAMAGES, DECLARATORY AND EQUITABLE RELIEF**<br><br>Courtroom: 6, 17th Floor<br>Judge: The Hon. Vaughn R. Walker<br><br>**DEMAND FOR JURY TRIAL** |

Dockets.Justia.com

Plaintiffs, by their attorneys, for their Master Consolidated Complaint against Defendants Transworld Network Corp., Comcast Telecommunications, Inc., T-Mobile USA, Inc., and McLeodUSA Telecommunications Services, Inc., allege, upon information and belief, as follows:

## PRELIMINARY STATEMENT

1. This Master Consolidated Complaint Against Defendants Transworld Network Corp ("Transworld")., Comcast Telecommunications, Inc. ("Comcast"), T-Mobile USA, Inc. ("T-Mobile"), and McLeodUSA Telecommunications Services, Inc. ("McLeod"), hereafter referred to as the Master Complaint, is filed pursuant to the Order of this Court and presents all federal constitutional and statutory claims brought against Defendants Transworld, Comcast, T-Mobile, and McLeod, ("Defendants"), in the separate cases transferred by the Panel on Multidistrict Litigation in this matter in its orders dated August 14, 2006, and September 25, 2006 ("transferred cases"). Unless otherwise ordered by this Court, all federal claims presented in any case against Defendants subsequently transferred to this Court by the Panel on Multidistrict Litigation in this matter shall be deemed to be included in this Master Complaint.

2. This Master Complaint is filed solely as an administrative device to promote judicial efficiency and economy in the adjudication and resolution of pretrial matters and is not intended to effect consolidation for trial of the transferred cases. Neither is this Master Complaint intended to cause, nor to change the rights of the parties, nor to make those who are parties in one transferred case parties in another.

3. This case challenges the legality of Defendants' participation in a secret and illegal government program to intercept and analyze vast quantities of Americans' telephone and Internet communications and records, surveillance done without any statutorily authorized permission, customers' knowledge or consent, or the authorization of a court, and in violation of

federal electronic surveillance and telecommunications statutes, as well as the First and Fourth Amendments to the United States Constitution. In addition, Plaintiffs challenge Defendant's conduct under state law.

## JURISDICTION AND VENUE

4. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1331, 28 U.S.C. § 1332(d), 18 U.S.C. § 2707, and 47 U.S.C. § 605. Supplemental jurisdiction over state law claims is founded on 28 U.S.C. § 1367.

5. Venue is proper in this District pursuant to the order of the Panel on Multidistrict Litigation.

## PARTIES

6. Plaintiff Travis Cross is an individual residing in Indianapolis, Indiana, and has been a subscriber and user of Comcast Telecommunications, Inc.'s Internet service for more than three years, and has used it to send and receive e-mail messages.

7. Plaintiffs Christopher and Rebecca Yowtz, husband and wife, reside in Coopersville, Michigan, and are subscribers and users of Transworld's telecommunications services, and have used them to make telephone or wireless calls and/or to send and receive Internet messages and e-mails.

8. Plaintiff Sam Goldstein is an individual residing in Indianapolis, Indiana, and has been a subscriber and user of McLeod's, long distance service since at least 2000 and has used it to make long distance telephone calls. Plaintiff Goldstein has also been a subscriber and user of Comcast's Internet service for at least two years and has used it to send and receive e-mail messages.

9. Plaintiff The Libertarian Party of Indiana is a political party with its central office located in Indianapolis, Indiana, and is a subscriber and user of McLeod's long distance

service, and has used it to make long distance telephone calls. The Libertarian Party of Indiana has a special interest in this action as Defendants' wrongful conduct affects its specially protected rights to political speech.

10. Plaintiff Carolyn W. Rader is an individual living in Indianapolis, Indiana, and has been a subscriber and user of MCE Communications Services, Inc. since 2001 and has used it to make telephone calls. Ms. Rader was previously a user and subscriber of T-Mobile's cellular phone services, and used it to make wireless calls. Ms. Rader has a special interest in this action in that she is a licensed attorney legally obligated to protect communications with her clients.

11. Plaintiff Sam Goldstein Insurance Agency, Inc. is a domestic corporation doing business in Indianapolis, Indiana, and has been a subscriber and user of McLeod's long distance service since at least 2000, and has used it to make long distance telephone calls. It has also been a user and subscriber to Comcast's Internet services for at least two years, and has used it to send and receive e-mail messages.

12. Plaintiff Sean Sheppard is an individual residing in Indianapolis, Indiana, and has been a subscriber and user of Comcast's Internet services for approximately four years and has used it to send and receive e-mail messages.

13. Defendant Transworld is a Minnesota corporation registered to do business in many states, including but not limited to the State of Michigan, and is a "telecommunication carrier" within the meaning of the Communications Act of 1934, 47 U.S.C. §§ 151, *et seq.* and provides remote computing and electronic communications services to the public.

14. Defendant Comcast is a Pennsylvania corporation registered to do business in many states, including but not limited to the State of Indiana, and is a "telecommunication

carrier" within the meaning of the Communications Act of 1934, 47 U.S.C. §§ 151, *et seq.* and provides remote computing and electronic communications services to the public.

15. Defendant McLeod is an Iowa corporation registered to do business in many states, including but not limited to the State of Indiana, and is a "telecommunication carrier" within the meaning of the Communications Act of 1934, 47 U.S.C. §§ 151, *et seq.* and provides remote computing and electronic communications services to the public.

16. Defendant T-Mobile is a Delaware corporation registered to do business in many states, including but not limited to the State of Indiana, and is a "telecommunication carrier" within the meaning of the Communications Act of 1934, 47 U.S.C. §§ 151, *et seq.* and provides remote computing and electronic communications services to the public.

**FACTUAL ALLEGATIONS**

17. In Section 222 of the Communications Act of 1934 (47 U.S.C. § 222(c)(1)), Congress imposed upon telecommunication carriers such as Defendants a duty to protect sensitive, personal customer information from disclosure. This information includes "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship" and data concerning service customers' telephone calling histories (*i.e.*, date, time, duration, and telephone numbers of calls placed or received) or call-detail records, and such information constitutes "individually identifiable customer proprietary network information" within the meaning of Section 222 of the Communications Act of 1934.

18. Federal law prohibits the federal government, which should be construed throughout this Master Complaint to include the National Security Agency ("NSA") and affiliated governmental agencies, from obtaining customers' call-detail records without a warrant, subpoena,

or other valid legal process, and similarly prohibits telecommunications providers, such as Defendants, from giving such information to the government without judicial or other lawful authorization, probable cause, and/or individualized suspicion.

19. Defendants Transworld, Comcast, T-Mobile, and McLeod, provide remote computing and electronic communication services to the public.

20. In the aftermath of September 11, 2001, the Defendants commenced their programs of providing the federal government with the telephone call contents and records of its customers and subscribers. The Defendants continue to provide this information to the federal government.

21. On December 16, 2005, in an article entitled "Bush Lets U.S. Spy on Callers Without Courts," *The New York Times* reported on an NSA program of eavesdropping on the telephone conversations of Americans without court order as required by the Foreign Intelligence Surveillance Act ("NSA Program").

22. In a December 17, 2005, radio address, President George W. Bush admitted that "[i]n the weeks following the terrorist attacks on our nation, [he] authorized the National Security Agency, consistent with U.S. law and the Constitution, to intercept the international communications of people with known links to al Qaeda and related terrorist organizations." President Bush further stated that "the activities [he] authorized are reviewed approximately every 45 days"; that he had "reauthorized this program more than 30 times since the September the 11th attacks"; and that he intended to continue authorizing such activity "for as long as our nation faces a continuing threat from al Qaeda and related groups."

23. In a press briefing on December 19, 2005, by Attorney General Alberto Gonzales and General Michael Hayden, Principal Deputy Director for National Intelligence, the government claimed that the NSA Surveillance Program targets communications between a party

outside the United States and a party inside the United States when one of the parties of the communication is believed to be "a member of al Qaeda, affiliated with al Qaeda, or a member of an organization affiliated with al Qaeda, or working in support of al Qaeda."

24. In a press release on December 19, 2005, Attorney General Alberto Gonzales stated that the Program involved "intercepts of contents of communications . . . ." While the Attorney General's description of the Program was limited to interception of communications with individuals "outside the United States," Attorney General Gonzales explained that his discussion was limited to those parameters of the program already disclosed by the President and that many other operational aspects of the program remained highly classified.

25. On December 24, 2005, *The New York Times* reported in an article entitled, "Spy Agency Mined Vast Data Trove, Officials Report," that:

> [t]he National Security Agency has traced and analyzed large volumes of telephone and Internet communications flowing into and out of the United States as part of the eavesdropping program that President Bush approved after the Sept. 11, 2001, attacks to hunt for evidence of terrorist activity, according to current and former government officials. The volume of information harvested from telecommunication data and voice networks, without court-approved warrants, is much larger than the White House has acknowledged, the officials said. It was collected by tapping directly into some of the American telecommunication system's main arteries, they said.

The officials said that as part of the program, "the N.S.A. has gained the cooperation of American telecommunications companies to obtain backdoor access to streams of domestic and international communications" and that the program is a "large data-mining operation" in which N.S.A. technicians have combed through large volumes of phone and Internet traffic in search of patterns that might point to terrorism suspects. *Id.* In addition, the article reports,

> "[s]everal officials said that after President Bush's order authorizing the N.S.A. program, senior government officials arranged with officials of some of the nation's largest telecommunications companies to gain access to switches that act as gateways at the borders between the United States' communication networks and international networks."

26. In a January 3, 2006, article entitled, “Tinker, Tailor, Miner, Spy” (available at http://www.slate.com/toolbar.aspx?action=print&id=2133564), Slate.com reported,

> “[t]he agency [the NSA] used to search the transmissions it monitors for key words, such as names and phone numbers, which are supplied by other intelligence agencies that want to track certain individuals. But now the NSA appears to be vacuuming up all data, generally without a particular phone line, name, or e-mail address as a target. Reportedly, the agency is analyzing the length of a call, the time it was placed, and the origin and destination of electronic transmissions.”

27. In a January 17, 2006, article, “Spy Agency Data After Sept. 11 Led F.B.I. to Dead Ends,” *The New York Times* stated that officials who were briefed on the N.S.A. program said that “the agency collected much of the data passed on to the F.B.I. as tips by tracing phone numbers in the United States called by suspects overseas, and then by following the domestic numbers to other numbers called. In other cases, lists of phone numbers appeared to result from the agency’s computerized scanning of communications coming into and going out of the country for names and keywords that might be of interest.”

28. A January 20, 2006, article in the *National Journal*, entitled “NSA Spy Program Hinges On State-Of-The-Art Technology,” reported that

> “[o]fficials with some of the nation’s leading telecommunications companies have said they gave the NSA access to their switches, the hubs through which enormous volumes of phone and e-mail traffic pass every day, to aid the agency’s effort to determine exactly whom suspected Qaeda figures were calling in the United States and abroad and who else was calling those numbers. The NSA used the intercepts to construct webs of potentially interrelated persons.”

29. In a January 21, 2006, article in *Bloomberg News* entitled “Lawmaker Queries Microsoft, Other Companies On NSA Wiretaps,” Daniel Berninger, a senior analyst at Tier 1 Research in Plymouth, Minnesota, said,

> “[i]n the past, the NSA has gotten permission from phone companies to gain access to so-called switches, high-powered computer into which phone traffic flows and is redirected, at 600 locations across the nation. . . . From these corporate relationships, the NSA can get the content of calls and records on their date, time, length, origin and destination.”

30. On February 5, 2006, an article appearing in the Washington Post entitled "Surveillance Net Yields Few Suspects" stated that officials said

> "[s]urveillance takes place in several stages . . . the earliest by machine. Computer-controlled systems collect and sift basic information about hundreds of thousands of faxes, e-mails and telephone calls into and out of the United States before selecting the ones for scrutiny by human eyes and hears. Successive stages of filtering grow more intrusive as artificial intelligence systems rank voice and data traffic in order of likeliest interest to human analysts."

The article continues,

> "[f]or years, including in public testimony by Hayden, the agency [the NSA] has acknowledged use of automated equipment to analyze the contents and guide analysts to the most important ones. According to one knowledgeable source, the warrantless program also uses those methods. That is significant . . . because this kind of filtering intrudes into content, and machines 'listen' to more Americans than humans do."

31. On February 6, 2006, in an article entitled "Telecoms Let NSA Spy On Calls," *USA Today* reported that "[t]he National Security Agency has secured the cooperation of large telecommunications companies, including AT&T, MCI and Sprint, in its efforts to eavesdrop without warrants on international calls by suspected terrorists, according to seven telecommunications executives." The article acknowledged that *The New York Times* had previously reported that the telecommunications companies had been cooperating with the government but had not revealed the names of the companies involved. In addition, it stated that long-distance carriers AT&T, MCI, and Sprint "all own 'gateway' switches capable of routing calls to points around the globe:

> "Decisions about monitoring calls are made in four steps, according to two U.S. intelligence officials familiar with the program who insisted on anonymity because it remains classified:
>
> - Information from U.S. or allied intelligence or law enforcement points to a terrorism-related target either based in the United States or communicating with someone in the United States.
> - Using a 48-point checklist to identify possible links to al-Qaeda, one of three NSA officials authorized to approve a warrantless intercept decides whether the surveillance is justified. Gen. Michael Hayden, the nation's No. 2 intelligence

officer, said the checklist focuses on ensuring that there is a 'reasonable basis' for believing there is a terrorist link involved.

- Technicians work with phone company officials to intercept communications pegged to a particular person or phone number. Telecommunications executives say MCI, AT&T, and Sprint grant the access to their systems without warrants or court orders. Instead, they are cooperating on the basis of oral requests from senior government officials.
- If the surveillance yields information about a terror plot, the NSA notifies the FBI or other appropriate agencies but does not always disclose the source of its information. Call-routing information provided by the phone companies can help intelligence officials eavesdrop on a conversation. It also helps them physically locate the parties, which is important if cell phones are being used. If the U.S. end of a communication has nothing to do with terrorism, the identity of the party is suppressed and the content of the communication destroyed, Hayden has said.

32. On May 11, 2006, in an article entitled "NSA Has A Massive Database Of Americans' Phone Calls," *USA Today* reported that "[t]he National Security Agency has been secretly collecting the phone call records of tens of millions of Americans, using data provided by AT&T, Verizon and Bellsouth," according to multiple sources with "direct knowledge of the arrangement." One of the confidential sources for the article reported that the NSA's goal is "to create a database of every call ever made" within the United States. The confidential sources reported that AT&T and the other carriers are working "under contract" with the NSA, which launched the program in 2001 shortly after the September 11, 2001 terrorist attacks. At the U.S. Senate confirmation hearing on his nomination to become Director of the Central Intelligence Agency, General Michael Hayden, who was the Director of the NSA at the time, confirmed that the program was "launched" on October 6, 2001.

33. The May 11, 2006, *USA Today* story was confirmed by a U.S. intelligence official familiar with the program. The story reports that the NSA requested that AT&T, SBC, and the other carriers "turn over their 'call-detail records,' a complete listing of the calling histories of their millions of customers," and provide the NSA with "updates" of the call-detail records. The confidential sources for the story reported that the NSA informed the carriers that it was willing to

pay for the cooperation, and that both "AT&T, which at the time was headed by C. Michael Armstrong," and "SBC, headed by Ed Whitacre," agreed to provide the NSA with the requested information.

34. The May 11, 2006, *USA Today* story reported that the NSA requested that Qwest Communications, Inc. ("Qwest"), another telecommunications carrier, provide the NSA with its customers' call-detail records, but Qwest refused. Qwest requested that the NSA first obtain a court order, a letter of authorization from the U.S. Attorney General's office, or permission from a Court operating under the Foreign Intelligence Surveillance Act ("FISA"), but the NSA refused, because it was concerned that the FISA Court and the Attorney General would find the NSA's request unlawful.

35. As of the date of the filing of this complaint, no part of the May 11, 2006, *USA Today* story has been publicly denied by any representative of the federal government, including the NSA.

36. Qwest's decision not to participate was also reported in an article from *The New York Times* on May 13, 2006, entitled, "Questions Raised For Phone Giants In Spy Data Furor." The article reported that Qwest's former CEO, Mr. Joseph Nacchio,

> "'made inquiry as to whether a warrant or other legal process had been secured in support of that request. When he learned that no such authority had been granted, and that there was a disinclination on the part of the authorities to use any legal process,' Mr. Nacchio concluded that the requests violated federal privacy requirements 'and issued instructions to refuse to comply.'"

37. Senator Christopher "Kit" Bond (R-MO), who also has received access to information on warrantless surveillance operations, explained on May 11, 2006, on a PBS Online NewsHour program entitled "NSA Wire Tapping Program Revealed" that "[t]he president's program uses information collected from phone companies . . . what telephone number called what other telephone number."

38. On May 14, 2006, when Senate Majority Leader William Frist (R-TN) was asked on CNN Late Edition with Wolf Blitzer whether he was comfortable with the program described in the *USA Today* article, he stated "Absolutely. I am one of the people who are briefed . . . I've known about the program. I am absolutely convinced that you, your family, our families are safer because of this particular program."

39. On May 29, 2006, Seymour Hersh reported in *The New Yorker* in an article entitled "Listening In" that a security consultant working with a major telecommunications carrier

> "told me that his client set up a top-secret high-speed circuit between its main computer complex and Quantico, Virginia, the site of a government-intelligence computer center. This link provided direct access to the carrier's network core – the critical area of its system, where all its data are stored. 'What the companies are doing is worse than turning over records,' the consultant said. 'They're providing total access to all the data.'"

40. A June 30, 2006, *USA Today* story reported that 19 members of the intelligence oversight committees of the U.S. Senate and House of Representatives "who had been briefed on the program verified that the NSA has built a database that includes records of Americans' domestic phone calls," and that four of the committee members confirmed that "MCI, the long-distance carrier that Verizon acquired in January, did provide call records to the government."

41. The Defendants knowingly and intentionally provided the aforementioned telephone contents and records to the federal government.

42. Upon information and belief, the NSA accomplishes its surveillance activities through the installation, maintenance and operation of various electronic routing and trapping equipment placed on the premises, or attached to the property, of Defendants to gain access to Defendants' stored databases of customer records and live electronic communication pathways ("NSA Program"). Such equipment, which provides the NSA with a direct tap into the

nations' telecommunication pipelines, would not have been installed, operated and/or maintained by the NSA absent cooperation, permission, and/or knowledge of the Defendants.

43. As part of the NSA Program, the NSA's operational personnel identify particular individual targets, and their communications, through a software data mining process that NSA runs against vast databases of the Defendants' stored electronic records of their customers' domestic and international telephone and Internet communications in search of particular names, numbers, words or phrases and patterns of interest. The NSA's operational personnel also identify communications of interest in real-time through similar data-mining software functionality.

44. Besides actually eavesdropping on specific conversations, NSA personnel have intercepted large volumes of domestic and international telephone and Internet traffic in search of patterns of interest, in what has been described in press reports as a large "data mining" program.

45. As part of this data-mining program, the NSA intercepts millions of communications made or received by people inside the United States, and uses powerful computers to scan their contents for particular names, numbers, words, or phrases.

46. Additionally, the NSA collects and analyzes a vast amount of communications traffic data to identify persons whose communications patterns the government believes may link them, even if indirectly, to investigatory targets.

47. The NSA has accomplished its massive surveillance operation by arranging with some of the nation's largest telecommunications companies to gain direct access to the telephone and Internet communications transmitted via those companies' domestic telecommunications facilities, and to those companies' records pertaining to the communications they transmit.

48. The Defendants have intercepted and continue to provide the government with direct access to all or a substantial number of the communications transmitted through its key domestic telecommunications facilities, including direct access to streams of domestic, international, and foreign telephone and Internet communications.

49. Since in or about October of 2001, the Defendants have disclosed and/or divulged the "call-detail records" of all or substantially all of their customers, including Plaintiffs, to the NSA, in violation of federal law, as more particularly set forth below.

50. The Defendants have, since in or about October 2001, been disclosing to the NSA "individually identifiable customer proprietary network information" belonging to all or substantially all of their customers, including, but not limited to, Plaintiffs, in violation of federal law, as more particularly set forth below.

51. The Defendants have disclosed and continue to disclose and/or provide the government with direct access to its databases of stored telephone and Internet records, which are updated with new information in real time or near-real time.

52. The Defendants have provided at all relevant times and continue to provide computer or storage processing services to the public, by means of wire, radio, electromagnetic, photo-optical, or photo-electronic facilities for the transmission of wire or electronic communications, and/or by means of computer facilities or related electronic equipment for the electronic storage of such communications.

53. The Defendants have knowingly authorized, and continue to knowingly authorize, NSA and affiliated governmental agencies to install and use, or have assisted government agents in installing or using, interception devices and pen registers and/or trap and trace devices on the Defendants' domestic telecommunications facilities in connection with the Program.

54. The interception devices and pen registers and/or trap and trace devices capture, record or decode the various information pertaining to individual class member communications including dialing, routing, addressing and/or signaling information ("DRAS information") for all or a substantial number of all wire or electronic communications transferred through the Defendants' domestic telecommunications facilities where those devices have been installed.

55. Using these devices, government agents have acquired and are acquiring wire or electronic communications content and DRAS information directly via remote or local control of the device.

56. In addition, or in the alternative, the Defendants have disclosed and are disclosing wire or electronic communications content and DRAS information to the government after interception, capture, recording or decoding.

57. The Defendants have knowingly authorized, and continue to knowingly authorize, the NSA and affiliated governmental agencies to directly access, through the installed devices, all domestic, international and foreign telephone and wireless telephone and Internet communications transmitted through the Defendants' domestic telecommunications infrastructure and facilities for use in the Program.

58. The Defendants provide the aforementioned telephone contents and records to the federal government without judicial or other lawful authorization, a court order, warrant, subpoena, statutory authorization, or certification pursuant to Chapters 119 and 121 of Title 18 of the United States Code, and records pertaining to their communications occurred without judicial or other lawful authorization, probable cause, and/or individualized suspicion.

59. The Defendants did not disclose to its customers, including plaintiffs, that it was providing the aforementioned telephone contents and records to the federal government. Thus,

the Defendants' customers, including plaintiffs, were not given the opportunity to, nor did they consent to the disclosure of their telephone contents and records.

60. The telephone contents and records intercepted and/or disclosed and/or divulged by the Defendants to the federal government pursuant to the program challenged herein were not divulged (a) pursuant to a law enforcement investigation concerning telemarketing fraud; (b) as a necessary incident to the rendition of services to customers; (c) to protect the rights or property of the Defendants; (d) based on a reasonable and/or good faith belief that an emergency involving danger of death or serious physical injury required disclosure without delay; (e) to the National Center for Missing and Exploited Children; or (f) to a non-governmental person or entity.

61. Defendants' violations were done with knowledge of the illegality, and therefore were made in bad faith.

## CLASS ACTION ALLEGATIONS

62. Plaintiffs brings this action under Federal Rule of Civil Procedure 23 on behalf of themselves and a Class, defined as:

> All individuals and entities located in the United States that have been subscribers or customers of Defendant's telephone, wireless or Internet services at any time since October 6, 2001. Excluded from the Class are Defendant, Defendant's predecessors, affiliates, parents, subsidiaries, officers and directors; all federal, state, and local governmental entities; any and all judges and justices assigned to hear any aspect of this litigation, their court staffs, their spouses, any minor children residing in their households, and any persons within the third degree of relationship to any judge or justice assigned to hear any aspect of this litigation.

63. Plaintiff seeks certification of the Class under Federal Rule of Civil Procedure 23(a), 23(b)(1), 23(b)(2), and 23(b)(3).

64. The Class number{s} in the millions, so that joinder of all members is impractical.

65. The claims of Plaintiffs are typical of the claims of the Class. Plaintiffs will fairly and adequately protect the interests of the Class. Plaintiffs have no conflicts with any other Class member, and have retained competent counsel experienced in class actions, consumer, telecommunications, and civil rights litigation.

66. Common questions of law and fact exist, including:

1. whether the Defendants disclosed and/or divulged its customers' telephone records [and content] to the federal government;
2. whether the Defendants violated federal law in disclosing and/or divulging its customers' telephone records and content to the federal government;
3. whether Plaintiffs are entitled to damages; and
4. whether Plaintiffs are entitled to equitable relief.

67. These and other questions of law and fact are common to the Class and predominate over any questions affecting only individual members.

68. A class action is a superior method for the fair and efficient adjudication of the controversy described herein. A class action provides an efficient and manageable method to enforce the rights of Plaintiffs and members of the Class.

69. The prosecution of separate actions by individual members of the Class would create a risk on inconsistent or varying adjudication, establishing incompatible standards of conduct for Defendants.

70. Defendants have acted, and refused to act, on grounds generally applicable to the Class, thereby making appropriate relief with respect to the Class as a whole.

**NECESSITY OF INJUNCTIVE RELIEF**

71. The named Plaintiffs and the members of the Class will continue in the future to use their telephones.

72. Unless this Court enjoins the Defendants' program challenged herein, the Defendants will continue to engage in the program.

73. The named Plaintiffs and the members of the Class will suffer irreparable harm as a result of the continuation of the Defendants' program, and they have no adequate remedy at law.

## CLAIMS FOR RELIEF

### FIRST CLAIM FOR RELIEF
### Violation of 18 U.S.C. §§ 2702(a)(1) and/or (a)(2)

74. Plaintiffs incorporate all of the allegations contained in the preceding paragraphs of this complaint, as if set forth fully herein.

75. In relevant part, 18 U.S.C. § 2702 provides that:

> a) Prohibitions. Except as provided in subsection (b) or (c)--
>
> (1) a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service; and
>
> (2) a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service--
>
> (A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service;
>
> (B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing. . . .

89. The Defendants knowingly divulged to one or more persons or entities the contents of Plaintiffs' communications while in electronic storage by a Defendant electronic

communication service, and/or while carried or maintained by a Telecom Defendant remote computing service, in violation of 18 U.S.C. §§ 2702(a)(1) and/or (a)(2).

91. The Defendants did not notify Plaintiffs of the divulgence of their communications, nor did Plaintiffs consent to such.

92. Neither the NSA nor any other governmental entity has obtained a warrant authorizing the disclosures, pursuant to 18 U.S.C. § 2703(c)(1)(A).

93. Neither the NSA nor any other governmental entity has obtained a court order authorizing the disclosures, pursuant to 18 U.S.C. § 2703(c)(1)(B) and (d).

94. Neither the NSA nor any other governmental entity has issued or obtained an administrative subpoena authorized by a federal or state statute authorizing such disclosures, pursuant to 18 U.S.C. § 2703(c)(1)(E) and (c)(2).

95. Neither the NSA nor any other governmental entity has issued or obtained a federal or state grand jury or trial subpoena authorizing such disclosures, pursuant to 18 U.S.C. § 2703(c)(1)(E) and (c)(2).

96. Defendants have not been provided with a certification in writing by a person specified in 18 U.S.C. § 2518(7) or by the Attorney General of the United States meeting the requirements of 18 U.S.C. § 2511(2)(a)(ii)(B), *i.e.*, a certification that no warrant or court order authorizing the disclosures is required by law, and that all statutory requirements have been met.

97. The disclosures were and are not authorized by any statute or legislation.

98. Defendants' disclosures in violation of 18 U.S.C. § 2702(a)(3) were and are knowing, intentional, and willful.

99. Defendants' continued engagement in the above-described divulgence of Plaintiffs' communications while in electronic storage by Defendants' electronic communication

service(s), and/or while carried or maintained by Defendants' remote computing service(s) represents a credible threat of immediate future harm.

100. Plaintiffs have been and are aggrieved by Defendants' above-described divulgence of the contents of their communications.

101. Pursuant to 18 U.S.C. § 2707, which provides a civil action for any person aggrieved by knowing or intentional violation of 18 U.S.C. § 2702, Plaintiffs seek such preliminary and other equitable or declaratory relief as may be appropriate; statutory damages of no less than $1000 for each aggrieved Plaintiff; punitive damages as the Court considers just, and reasonable attorneys' fees and other litigation costs reasonably incurred.

**SECOND CLAIM FOR RELIEF**
**Violation of 18 U.S.C. § 2702(a)(3)**

102. Plaintiffs incorporate all of the allegations contained in the preceding paragraphs of this complaint, as if set forth fully herein.

103. In relevant part, 18 U.S.C. § 2702 provides that:

> (a) Prohibitions. – Except as provided in subsection . . . (c) –
> (3) a provider of . . . electronic communication service to the public shall not knowingly divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by paragraph (1) or (2) to any governmental entity.

104. Defendants' telephone services are "electronic communication service[s]," as that term is defined in 18 U.S.C. § 2510(15), provided to the public, including Plaintiffs.

105. The Defendants violated 18 U.S.C. § 2702(a)(3) by knowingly and intentionally divulging to the federal government records or other information pertaining to subscribers or customers of the Defendants' remote computing and electronic services.

106. The Defendants' challenged program of disclosing telephone records to the federal government does not fall within any of the statutory exceptions or immunities set forth in 18 U.S.C. §§ 2702(c), 2703(c), or 2703(e).

107. Neither the NSA nor any other governmental entity has obtained a warrant authorizing the disclosures, as is required by 18 U.S.C. § 2703(c)(1)(A).

108. Neither the NSA nor any other governmental entity has obtained a court order authorizing the disclosures, as is required by 18 U.S.C. § 2703(c)(1)(B) and (d).

109. Neither the NSA nor any other governmental entity has issued or obtained an administrative subpoena authorized by any federal or state statute authorizing such disclosures, as is required by 18 U.S.C. § 2703(c)(1)(E) and (c)(2).

110. Neither the NSA nor any other governmental entity has issued or obtained a federal or state grand jury or trial subpoena authorizing such disclosures, as is required by 18 U.S.C. § 2703(c)(1)(E) and (c)(2).

111. Defendants have not been provided with a certification in writing by a person specified in 18 U.S.C. § 2518(7), by the Director of the Federal Bureau of Investigation or his designee or a Special Agent in Charge in a Bureau field office pursuant to 18 U.S.C. § 2709(b), or by the Attorney General of the United States to meet the requirements of 18 U.S.C. § 2511(2)(a)(ii)(B), *i.e.*, certifying that no warrant or court order authorizing the disclosures is required by law, and that all statutory requirements have been met.

112. The disclosures were and continue to be unauthorized by any statute or legislation.

113. Plaintiffs have been and continue to be aggrieved by the Defendants' knowing and intentional past disclosure and/or imminent future disclosure of their records to the

federal government. Accordingly, Plaintiffs may challenge this violation of 18 U.S.C. § 2702(a)(3) pursuant to the cause of action created by 18 U.S.C. § 2707(a).

**THIRD CLAIM FOR RELIEF**
**Violation of 18 U.S.C. §§ 2511(1)(a), (1)(c), (1)(d), and (3)(a)**

114. Plaintiffs incorporate all of the allegations contained in the preceding paragraphs of this complaint, as if set forth fully herein.

115. In relevant part, 18 U.S.C. § 2511 provides that:

> (1) Except as otherwise specifically provided in this chapter, any person who –
>
> (a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral or electronic communication. . . .
>
> (c) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection;
>
> (d) intentionally uses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection. . . . .
>
> (3)(a) Except as provided in paragraph (b) of this subsection, a person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication (other than one to such person or entity, or an agent thereof) while in transmission on that service to any person or entity other than addressee or intended recipient of such communication or an agent of such addressee or intended recipient.

116. The Defendants violated 18 U.S.C. §§ 2511(1)(a), (1)(c), (1)(d), and (3)(a) by intentionally intercepting and disclosing to the federal government the contents of telephone calls of the Defendants' customers.

117. The Defendants violated 18 U.S.C. § 2511(1)(d) by intentionally using, or endeavoring to use, the contents of Plaintiffs' wire or electronic communications, with knowledge or reason to know that the information was obtained through the interception of wire or electronic communications.

118. The Defendants' challenged program of intercepting and disclosing the contents of telephone calls to the federal government does not fall within any of the statutory exceptions or immunities set forth in 18 U.S.C. §§ 2511(2), 2511(3)(b), or 2520(d).

119. Plaintiffs have been and continue to be aggrieved by the Defendants' intentional past and/or imminent future interception and disclosure of telephone call contents to the federal government. Accordingly, Plaintiffs may challenge this violation of 18 U.S.C. §§ 2511(1)(a), (1)(c), (1)(d) and (3)(a) pursuant to the cause of action created by 18 U.S.C. § 2520(a).

## FOURTH CLAIM FOR RELIEF
## Violation of 47 U.S.C. § 605

120. Plaintiffs incorporate all of the allegations contained in the preceding paragraphs of this complaint, as if set forth fully herein.

121. In relevant part, 47 U.S.C. § 605 provides that:

(a) Practices prohibited –

> Except as authorized by chapter 119, Title 18, no person receiving, assisting in receiving, transmitting, or assisting in transmitting, any interstate or foreign communication by wire or radio shall divulge or publish the existence . . . thereof, except through authorized channels of transmission or reception, (1) to any person other than the addressee, his agent, or attorney, (2) to a person employed or authorized to forward such communication to its destination, (3) to proper accounting or distributing officers of the various communicating centers over which the communication may be passed, (4) to the master of a ship under whom he is serving, (5) in response to a subpoena issued by a court of competent jurisdiction, or (6) on demand of other lawful authority.

122. The Defendants received, assisted in receiving, transmitted, or assisted in transmitting, Plaintiffs' interstate communications by wire.

123. The Defendants violated 47 U.S.C. § 605 by divulging or publishing the "existence" of Plaintiffs' communications to the federal government, by means other than through authorized channels of transmission or reception. The Defendants' disclosure and publication of the existence of Plaintiffs' communications was not authorized by any provision of 18 U.S.C. §§ 2510-2522.

124. Defendants' disclosure and publication of the existence and contents of Plaintiffs' and Class members' communications was willful and in bad faith and for purposes of direct or indirect commercial advantage or private financial gain, as they were paid for their cooperation, and a failure to cooperate might have jeopardized their ability to obtain lucrative government contracts.

125. The Defendants failed to notify Plaintiff or Class members of the Defendant's disclosure and/or publication of the existence of Plaintiffs' communications, nor did Plaintiffs consent to such disclosure and publication.

126. Pursuant to 47 U.S.C. § 605(e)(3), Plaintiffs seek: (a) a declaration that the disclosures are in violation of 47 U.S.C. § 605(a); (b) a preliminary injunction restraining Defendants from continuing to make such unlawful disclosures; (c) a permanent injunction restraining Defendants from continuing to make such unlawful disclosures; (d) statutory damages of not less than $1,000 or more than $10,000 for each violation, plus, in the Court's discretion, an increase in the statutory damages of up to $100,000 for each violation; and (e) reasonable attorneys' fees and reasonable costs of this litigation.

## FIFTH CLAIM FOR RELIEF
## Violation of 50 U.S.C. § 1809

127. Plaintiffs repeat and incorporate herein by reference the allegations in the preceding paragraphs of this complaint, as if set forth fully herein.

128. In relevant part, 50 U.S.C. §1809 provides that:

> (a) Prohibited activities - A person is guilty of an offense if he intentionally - (1) engages in electronic surveillance under color of

> law except as authorized by statute; or (2) discloses or uses information obtained under color of law by electronic surveillance, knowing or having reason to know that the information was obtained through electronic surveillance not authorized by statute.

129. In relevant part 50 U.S.C. §180l provides that:

> (f) "Electronic surveillance" means - (1) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication sent by or intended to be received by a particular, known United States person who is in the United States, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes; (2) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States, but does not include the acquisition of those communications of computer trespassers that would be permissible under section 2511 (2)(i) of Title 18; (3) the intentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States; or (4) the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from a wire or radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes.

130. The Defendants have intentionally acquired, by means of a surveillance device, the contents of one or more telephone, wireless or Internet communications to or from Plaintiffs or other information in which Plaintiffs have a reasonable expectation of privacy, without the consent of any party thereto, and such acquisition occurred in the United States.

131. By the acts alleged herein, the Defendants have intentionally engaged in electronic surveillance (as defined by 50 U.S. C. §1801(f)) under color of law, but which is not authorized by any statute, and the Defendants have intentionally subjected Plaintiffs to such electronic surveillance, in violation of 50 U.S.C. §1809.

132. Additionally or in the alternative, by the acts alleged herein, the Defendants have intentionally disclosed or used information obtained under color of law by electronic surveillance, knowing or having reason to know that the information was obtained through electronic surveillance not authorized by statute.

133. The Defendants did not notify Plaintiffs of the above-described electronic surveillance, disclosure, and/or use, nor did Plaintiffs consent to such.

134. The Defendants' challenged program of electronic surveillance does not fall within any of the statutory exceptions or immunities set forth in 50 U.S.C. § 1809(b).

135. Defendants' continued engagement in the above-described electronic surveillance, disclosure, and/or use of Plaintiffs' electronic communications described herein, and that likelihood represents a credible threat of immediate future harm.

136. Plaintiffs have been and continue to be aggrieved by the Defendants electronic surveillance, disclosure, and/or use of their wire communications.

137. Pursuant to 50 U.S.C. §1810, which provides a civil action for any person who has been subjected to an electronic surveillance or about whom information obtained by electronic surveillance of such person has been disclosed or used in violation of 50 U.S.C. §1809, Plaintiffs seek equitable and declaratory relief; statutory damages for each Plaintiff and class member of whichever is the greater of $100 a day for each day of violation or $1,000; punitive damages as appropriate; and reasonable attorneys' fees and other litigation costs reasonably incurred.

## SIXTH CLAIM FOR RELIEF
## Violation of the First and Fourth Amendments
## to the United States Constitution

138. Plaintiffs incorporate all of the allegations contained in the preceding paragraphs of this complaint, as if set forth fully herein.

139. Plaintiffs have a reasonable expectation of privacy in their communications, contents of communications, and/or records pertaining to their communications transmitted, collected, and/or stored by the Defendants, which was violated by the Defendants' above-described actions as agents of the government, which constitute a search and seizure of Plaintiffs' communications and records.

140. Plaintiffs use the Defendants' services to speak or receive speech anonymously and to associate privately.

141. The above-described acts of interception, disclosure, divulgence and/or use of Plaintiffs' communications, contents of communications, and records pertaining to their communications occurred without judicial or other lawful authorization, probable cause, and/or individualized suspicion.

142. At all relevant times, the federal government instigated, directed, and/or tacitly approved all of the above-described acts of the Defendants.

143. At all relevant times, the federal government knew of and/or acquiesced in all of the above-described acts of the Defendants, and failed to protect the First and Fourth Amendment rights of the Plaintiffs by obtaining judicial authorization.

144. In performing the acts alleged herein, the Defendants had at all relevant times a primary or significant intent to assist or purpose of assisting the government in carrying out the Defendants' program and/or other government investigations, rather than to protect its own property or rights.

145. By the acts alleged herein, the Defendants acted as instruments or agents of the government, and thereby violated Plaintiffs' reasonable expectations of privacy and denied Plaintiffs their right to be free from unreasonable searches and seizures as guaranteed by the Fourth

Amendment to the Constitution of the United States, and additionally violated Plaintiffs' rights to speak and receive speech anonymously and associate privately under the First Amendment.

146. By the acts alleged herein, the Defendants' conduct proximately caused harm to Plaintiffs.

147. The Defendants' conduct was done intentionally, with deliberate indifference, or with reckless disregard of, Plaintiffs' constitutional rights.

## SEVENTH CLAIM FOR RELIEF
## Violation of State Surveillance Statutes

120. Plaintiffs repeat and incorporate herein by reference the allegations in the preceding paragraphs of this complaint, as if set forth fully herein.

121. Plaintiffs further state that Defendants have engaged and continue to engage in the unlawful eavesdropping, surveillance, and/or interception of wire, oral, and/or electronic communications, the disclosure and/or divulgence and/or use of the contents of such communications, and/or the unlawful installation and/or use of pen registers or trap and trace devices.

122. The foregoing conduct violates the following state statutes:

a. Ala. Code §§ 13A-11-30, 13A-11-31 (2006)
b. Alaska Stat. § 42.20.310 (2005)
c. Ariz. Rev. Stat. Ann. § 13-3005 (2006)
d. Ark. Code Ann. § 5-60-120 (2005)
e. Cal. Penal Code § 630 et seq. (2006)
f. Colo. Rev. Stat. §§ 18-9-301, 18-9-303 (2006)
g. Conn. Gen. Stat. § 52-570d (2006)
h. Del. Code Ann. Tit. 11, § 2402 (2005)
i. D.C. Code §§ 23-541, 23-542 (2006)
j. Fla. Stat. §§ 934.01-03 (2005)
k. Ga. Code Ann. §§ 16-11-62 et seq. (2005)

l. Haw. Rev. Stat. § 803-42, 803-48 (2005)

m. Idaho Code Ann. § 18-6702 (2005)

n. 720 Ill. Comp. Stat. 5/14-1, -2 (2006)

o. Ind. Code § 35-33.5-1 et seq. (2005)

p. Iowa Code § 727.8 (2005)

q. Kan. Stat. Ann. §§ 21-4001, 21-4002 (2004)

r. Ky. Rev. Stat. Ann. §§ 526.010-.020 (2005)

s. La. Rev. Stat. Ann. § 15:1303 (2005)

t. Me. Rev. Stat. Ann. Tit. 15, §§ 709-710 (2006)

u. Md. Code Ann. Cts. & Jud. Proc. § 10-402 et seq.; § 10-4A-4B et seq. (2006)

v. Mass. Gen. Laws ch. 272, § 99 (2006)

w. Mich. Comp. Laws § 750.539 et seq. (2006)

x. Minn. Stat. §§ 626A.01, .02 (2005)

y. Miss. Code Ann. § 41-29-501 et seq. (2006)

z. Mo. Rev. Stat. §§ 392.170, .350, 542.402, .418 (2006)

aa. Mont. Code Ann. § 45-8-213 (2006)

bb. Neb. Rev. Stat. § 86-290 (2006)

cc. Nev. Rev. Stat. 200.610-.620 (2006)

dd. N.H. Rev. Stat. Ann. §§ 570-A:1, -A:2 (2005)

ee. N.J. Stat. Ann. § 2A:156A-1 et seq. (2006)

ff. N.M. Stat. § 30-12-1 (2006)

gg. N.Y. Penal Law §§ 250.00, .05 (2006)

hh. N.C. Gen. Stat. § 15A-287 (2006)

ii. N.D. Cent. Code § 12.1-15-02 (2006)

jj. Ohio Rev. Code Ann. § 2933.51 et seq. (2006)

kk. Okla. Stat. tit. 13, § 176.1 et seq. (2006)

ll. Or. Rev. Stat. §§ 165.540, .543 (2006)

mm. 18 Pa. Cons. Stat. § 5701 et seq. (2005)

nn. R.I. Gen. Laws § 11-35-21 (2005)

oo. S.C. Code Ann. §§ 17-30-20, -30 (2005)

pp. S.D. Codified Laws §§ 23A-35A-1, 23A-35A-20 (2006)

qq. Tenn. Code Ann. § 39-13-601 (2006)

rr. Tex. Penal Code Ann. § 16.02 et seq.; Tex. Code Crim. Proc. art. 18.20 § 16(a) (2005)

ss. Utah Code Ann. § 77-23a-1 et seq. (2005)

tt. Va. Code Ann. §§ 19.2-61, -62 (2006)

uu. Wash. Rev. Code § 9.73.030 (2006)

vv. W. Va. Code § 62-1D-1 et seq. (2006)

ww. Wis. Stat. §§ 968.27, .31 (2005)

xx. Wyo. Stat. Ann. §§ 7-3-701, -702 (2005)

**EIGHTH CLAIM FOR RELIEF**
**Violations of the State Consumer Protection Statutes**

159. Plaintiffs incorporate all of the allegations contained in the preceding paragraphs of this complaint, as if set forth fully herein.

160. Plaintiffs further state that Defendants have violated and continue to violate state consumer protection statutes by divulging records or other information pertaining to subscribers and customers to a governmental entity, specifically the NSA, without Plaintiffs' knowledge or consent.

161. The unfair and deceptive trade acts and practices of Defendants directly, foreseeably, and proximately cause damages and injury to Plaintiff and the Class.

162. The actions and failures to act of Defendants, including the false and misleading representations and omissions of material facts regarding the protection and use of Class members' private information constitute an unfair method and unfair and/or deceptive acts in violation of the following state consumer protection statutes:

a) Defendants engage in unfair competition or deceptive acts or practices in violation of Ala. Code § 8-19-1 et seq.;

b) Defendants engage in unfair competition or deceptive acts or practices in violation of Alaska Stat. § 45.50.531(a);

c) Defendants engage in unfair competition or deceptive acts or practices in violation of Ariz. Rev. Stat. § 44-1522 et seq.;

d) Defendants engage in unfair competition or deceptive acts or practices in violation of Ark. Code § 4-88-101 et seq.;

e) Defendants engage in unfair competition or deceptive acts or practices in violation of Cal. Bus. & Prof. Code § 17200 et seq.;

f) Defendants engage in unfair competition or deceptive acts or practices or has made false representations in violation of Colo. Rev. Stat. § 6-1-105 et seq.;

g) Defendants engage in unfair competition or deceptive acts or practices in violation of Conn. Gen. Stat. § 42-110b et seq.;

h) Defendants engage in unfair competition or deceptive acts or practices in violation of 6 Del. Code § 2511 et seq.;

i) Defendants engage in unfair competition or deceptive acts or practices or made false representations in violation of D.C. Code Ann. § 28-3901 et seq.;

j) Defendants engage in unfair competition or deceptive acts or practices in violation of Fla. Stat. § 501.201 et seq.;

k) Defendants engage in unfair competition or deceptive acts or practices in violation of Ga. Stat. § 10-1-392 et seq.;

l) Defendants engage in unfair competition or deceptive acts or practices in violation of Haw. Rev. Stat. § 480 et seq.;

m) Defendants engage in unfair competition or deceptive acts or practices in violation of Idaho Code § 48-601 et seq.;

n) Defendants engage in unfair competition or deceptive acts or practices in violation of 815 Ill. Comp. Stat. § 505.1 et seq.;

o) Defendants engage in unfair competition or deceptive acts or practices in violation of Ind. Code § 24-5-0.5 et seq.;

p) Defendants engage in unfair competition or deceptive acts or practices in violation of Iowa Code § 714.16 et seq.;

q) Defendants engage in unfair competition or deceptive acts or practices in violation of Kan. Stat. Ann. § 50-623 et seq.;

r) Defendants engage in unfair competition or deceptive acts or practices in violation of Ky. Rev. Stat. § 367.1 10 et seq.;

s) Defendants engage in unfair competition or deceptive acts or practices in violation of La. Rev. Stat. § 51:1401 et seq.;

t) Defendants engage in unfair competition or deceptive acts or practices in violation of 5 Me. Rev. Stat. Ann. § 207 et seq.;

u) Defendants engage in unfair competition or deceptive acts or practices in violation of Massachusetts General Laws Ch. 93A et seq.;

v) Defendants engage in unfair competition or deceptive acts or practices in violation of Md. Com. Law Code § 13-101 et seq.

w) Defendants engage in unfair competition or deceptive acts or practices in violation of Mich. Stat. § 445.901 et seq.;

x) Defendants engage in unfair competition or deceptive acts or practices in violation of Minn. Stat. § 8.31 et seq.;

y) Defendants engage in unfair competition or deceptive acts or practices in violation of Miss. Code Ann. § 75-24-1 et seq.;

z) Defendants engage in unfair competition or deceptive acts or practices in violation of Mo. Ann. Stat. § 407.010 et seq.;

aa) Defendants engage in unfair competition or deceptive acts or practices in violation of Mont. Code § 30-14-101 et seq.;

bb) Defendants engage in unfair competition or deceptive acts or practices in violation of Neb. Rev. Stat. § 59-1601 et seq.;

cc) Defendants engage in unfair competition or deceptive acts or practices in violation of Nev. Rev. Stat. § 598.0903 et seq.;

dd) Defendants engage in unfair competition or deceptive acts or practices in violation of N.H. Rev. Stat. § 358-A:1 et seq.;

ee) Defendants engage in unfair competition or deceptive acts or practices in violation of violation of N.J. Rev. Stat. § 56:8-1 et seq.;

ff) Defendants engage in unfair competition or deceptive acts or practices in violation of N.M. Stat. § 57-12-1 et seq.;

gg) Defendants engage in unfair competition or deceptive acts or practices in violation of N.Y. Gen. Bus. Law § 349 et seq.;

hh) Defendants engage in unfair competition or deceptive acts or practices in violation of N.C. Gen. Stat. § § 75-1.1 et seq.;

ii) Defendants engage in unfair competition or deceptive acts or practices in violation of N.D. Cent. Code § 51-15-01 et seq.;

jj) Defendants engage in unfair competition or deceptive acts or practices in violation of Ohio Rev. Stat. § 1345.01 et seq.;

kk) Defendants engage in unfair competition or deceptive acts or practices in violation of Okla. Stat. 15 § 751 et seq.;

ll) Defendants engage in unfair competition or deceptive acts or practices in violation of Or. Rev. Stat. § 646.605 et seq.;

mm) Defendants engage in unfair competition or deceptive acts or practices in violation of 73 Pa. Stat. § 201-1 et seq.;

nn) Defendants engage in unfair competition or deceptive acts or practices in violation of R.I. Gen. Laws § 6-13.1-1 et seq.;

oo) Defendants engage in unfair competition or deceptive acts or practices in violation of S.C. Code Laws § 39-5-10 et seq.;

pp) Defendants engage in unfair competition or deceptive acts or practices in violation of S.D. Code Laws § 37-241 et seq.;

qq) Defendants engage in unfair competition or deceptive acts or practices in violation of Tenn. Code Ann. § 47-18-101 et seq.;

rr) Defendants engage in unfair competition or deceptive acts or practices in violation of Tex. Bus. & Com. Code § 17.41 et seq.;

ss) Defendants engage in unfair competition or deceptive acts or practices in violation of Utah Code § 13-11-1 et seq.;

tt) Defendants engage in unfair competition or deceptive acts or practices in violation of 9 Vt. Stat. § 2451 et seq.;

uu) Defendants engage in unfair competition or deceptive acts or practices in violation of Va. Code § 59.1-196 et seq.;

vv) Defendants engage in unfair competition or deceptive acts or practices in violation of Wash. Rev. Code § 19.86.010 et seq.;

ww) Defendants engage in unfair competition or deceptive acts or practices in violation of W. Va. Code § 46A-6-101 et seq.;

xx) Defendants engage in unfair competition or deceptive acts or practices in violation of Wis. Stat. § 100.18 et seq.; and

yy) Defendants engage in unfair competition or deceptive acts or practices in violation of Wyo. Stat. Ann. § 40-12-101 et seq.

163. This injury is of the type the state consumer protection and deceptive practices statutes were designed to prevent and directly results from Defendants' unlawful conduct.

**NINTH CLAIM FOR RELIEF**
**Unlawful and Unfair Business Practices in Violation of the**
**State Law**

164. Plaintiffs incorporate all of the allegations contained in the preceding paragraphs of this complaint, as if set forth fully herein.

165. By engaging in the acts and practices described herein, Defendants have engaged in unlawful and unfair business practices in violation of California's Unfair Competition Law, Business & Professions Code §§ 17200, *et seq.*

166. Defendants' acts and practices are unlawful because, as described above, they violate 47 U.S.C. § 222, 18 U.S.C. §§ 2702(a)(1), (a)(2), and (a)(3), 18 U.S.C. §§ 2511(1)(a), (1)(c), (1)(d), and (3)(a), 40 U.S.C. § 1809, and 47 U.S.C. § 605.

167. Defendants' acts and practices are also unlawful because they violate 18 U.S.C. § 3121. In relevant part, 18 U.S.C. § 3121 provides that:

> In general. – Except as provided in this section, no person may install or use a pen register or a trap and trace device without first obtaining a court order under section 3123 of this title or under the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 *et seq.*).
>
> As defined by 18 U.S.C. § 3127:
>
> (3) the term "pen register" means a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information

> shall not include the contents of any communication, but such term does not include any device or process used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services provided by such provider or any device or process used by a provider or customer of a wire communication service for cost accounting or other like purposes in the ordinary course of its business;
>
> (4) the term "trap and trace device" means a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication . . . .

168. Defendants have installed or used pen registers and/or trap and trace devices without first obtaining a valid court order under 18 U.S.C. § 3123 or a subpoena.

169. The pen registers and/or trap and trace devices installed and used by Defendants have captured, recorded, or decoded, and continue to capture, record or decode, dialing, routing, addressing or signaling information pertaining to Plaintiffs and/or California Subclass members' telephone, wireless**,** and Internet communications.

170. Defendants did not notify Plaintiff or California Subclass members of the installation or use of pen registers and/or trap and trace devices. Plaintiff and California Subclass members have not consented to Defendants' installation or use of pen registers and/or trap and trace devices.

171. Defendants are telecommunications carriers that obtain and have obtained customer proprietary network information by virtue of its provision of telecommunications service.

172. Defendants used and/or disclosed to the NSA, a government entity, individually identifiable customer proprietary network information pertaining to Plaintiffs and California Subclass members.

173. Defendants failed to notify Plaintiffs or California Subclass members of the disclosure and/or divulgence of their personally identifiable customer proprietary network information to the NSA, nor did Plaintiff or California Subclass members consent to such.

174. Defendants' acts and practices also constitute unfair business practices in violation of California's Unfair Competition Law, Business & Professions Code §§ 17200, *et seq.*,

because they contravene Defendant's privacy policy, which assures Plaintiffs and California Subclass members that information pertaining to their telephone calls and/or Internet communications will not be disclosed to third parties absent a valid court order or subpoena.

175. In violation of this policy and in breach of its trust with Plaintiffs and Class members, including the California Subclass Members, Defendants disclosed the customer proprietary network information belonging to Plaintiffs and the California Subclass, *i.e.*, their call-detail records, to the NSA without a court order or subpoena.

176. Plaintiffs and the California Subclass seek restitution, injunctive relief, and all other relief available under §§ 17200, *et seq.*]

**TENTH CLAIM FOR RELIEF**
**Breach of Contract**

177. Plaintiffs incorporate all of the allegations contained in the preceding paragraphs of this complaint, as if set forth fully herein.

178. At all times relevant herein, Defendants agreed to provide for a subscription fee, and Plaintiffs agreed to purchase from the Defendants various telecommunication and electronic communication services.

179. At all times relevant herein, Defendants impliedly and expressly promised to protect the privacy and confidentiality of its customers' information, identity, records, subscription, use details, and communications, and, to abide by federal and state law.

180. At all times relevant herein, Defendants by their conduct as alleged, breach their contract with the Plaintiffs, and breached the implied covenant of good faith and fair dealing as well.[1]

181. As a result of Defendants' breach of contractual duties owed to the Plaintiff, Defendants are liable for damages including, but limited to nominal and consequential damages.

[1] Plaintiffs preserve such claims with respect to states where breach of the implied covenant of good faith and fair dealing is plead separately.

## PRAYER FOR RELIEF

WHEREFORE, Plaintiffs on behalf of themselves and for all others similarly situated, respectfully requests that the Court:

A. Declare that Defendant's conduct as alleged herein violates applicable law;

B. Award statutory damages to Plaintiff and the Class;

C. Award punitive damages to Plaintiff and the Class;

D. Award Plaintiff's reasonable attorneys' fees and costs of suit;

E. Award restitution and all other relief allowed under State law claims

F. Enjoin Defendant's continuing violations of applicable law; and

Grant such other and further relief as the Court deems just and proper.

Dated: January 16, 2007

Respectfully submitted,

MOTLEY RICE LLC

/s/ Ronald L. Motley______________

Ronald L. Motley, Esq. (SC Bar No. RM-2730)
Jodi W. Flowers, Esq. (SC Bar No. 66300)
Donald Migliori, Esq. (RI Bar No. 4936;
MA Bar No. 567562; and MN Bar No. 0245951)
Vincent I. Parrett (CA Bar No. 237563)
28 Bridgeside Boulevard
P.O. Box 1792
Mount Pleasant, South Carolina 29465
Telephone: (843) 216-9000
Facsimile: (843) 216-9027

**INTERIM CLASS COUNSEL**

I, Shana E. Scarlett, am the ECF User whose ID and password are being used to file this Master Consolidated Complaint Against Transworld Network Corp., et al. In compliance with General Order 45, X.B., I hereby attest that Ronald L. Motley has concurred in this filing.

CERTIFICATE OF SERVICE

I hereby certify that on January 16, 2007, I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system which will send notification of such filing to the e-mail addresses denoted on the attached Electronic Mail Notice List.

/s/

SHANA E. SCARLETT

LERACH COUGHLIN STOIA GELLER RUDMAN & ROBBINS LLP
100 Pine Street, 26th Floor
San Francisco, CA 94111
Telephone: 415/288-4545
415/288-4534 (fax)
E-mail:shanas@lerachlaw.com